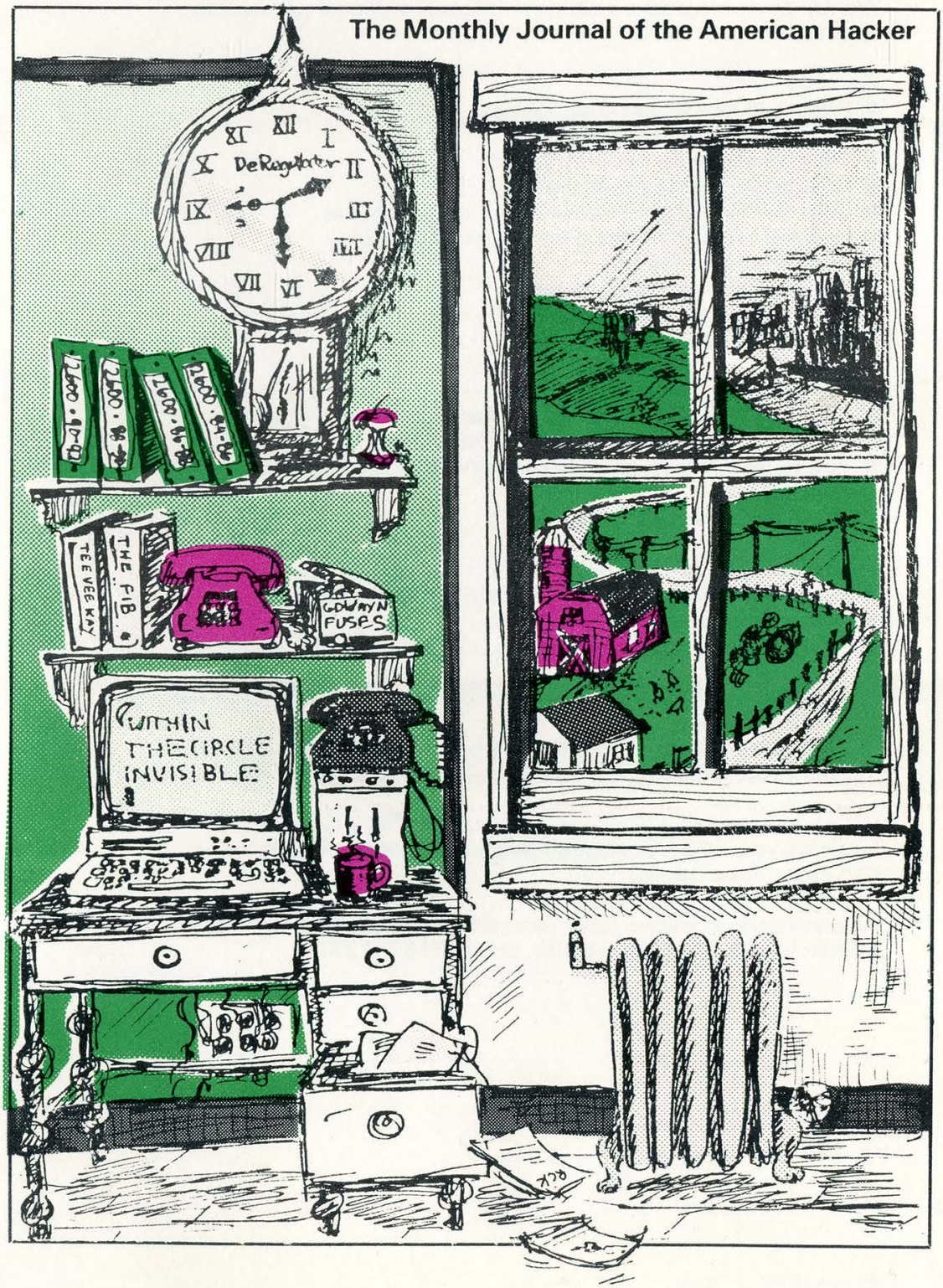
2600

Volume 4, Number 2 February, 1987 $2

The Monthly Journal of the American Hacker



2600 WANTS YOU!

Join the staff of 2600. It is simple.
Just compile any information you have so it is easily understandable and send it to us. We accept hardcopy and uploads. We will also accept information on floppies—call us if you wish to do that.

We need:
- Profiles of long distance companies
- Profiles of computer systems
- Reviews of popular security devices
- Lists of interesting phone numbers
- Lists of interesting reference books and magazines
- Updated tutorials on using things like ADS, CNA
- Interesting true stories
- Data that can be a good reference
- Maps of computer networks
- Analysis of new legislation

We would like:
- ***Legitimate access to various computer networks***
- ***You to continue to send your comments and questions***
- ***You to continue to send clippings from local papers and magazines***
- ***You to help keep us informed***

Things we could always use:
- ★ Printers, computers, telephones, and interesting devices
- ★ More modernized office equipment
- ★ A 2400 baud modem

If you send an article or data, please request a by-line otherwise we will not print one.
If you send us hardware, please make sure it is not stolen. We do not want your troubles.

We pay our writers a small amount. Perhaps that will be the incentive you need. We also pay people who get advertising for us. Call us for more details.

All contributors, please send your gifts to: 2600, P.O. Box 99, Middle Island, NY 11953-0099, or call 5167512600.

We've been swamped with mail from people who either wanted to renew at the old rate or who wanted to comment on our new style. Please forgive us if we seem to take a little longer to process your particular request—this avalanche far outweighed our wildest dreams.

This probably means we're doing quite well, but it's always hard to be conclusive. Our experiments with several newstands across the country appears to be succeeding as well, and we hope to have a distributor before long. Before long, 2600 will be a household word. Look for a list of newstands we can be found at in a future issue.

This month we're happy to present an exclusive interview with one of Britain's most notorious hackers, Hugo Cornwall. It's one of many we'll be presenting and we think there's a lot to be learned from his observations.

We've also got an article on COSMOS that many readers will no doubt fail to understand entirely. This has always been a problem for us here as we must constantly try to please both the beginners and the advanced hackers among us. One thing we believe everyone can get out of this article is a realization of all of the different ways your phone service can be categorized and how easy it is to change this with a simple stroke of the keyboard. It might lend some insight as to why you didn't get what you asked for or perhaps how you managed to wind up with a prison phone line.

Phones and computers are incredible and the two together can be quite scary. The purpose of our magazine is to show you what's going on with both—in as many ways as possible.

STAFFBOX

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Office Manager
Helen Victory

PSOS Operations
Tom Blich

Writers: John Drake, Paul Estev, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Bill from RNOC, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

Artists: Dan Holder, Mike Marshall, Tish Valter Koch.

2600 (ISSN 0749-3851) is published monthly by 2600 Enterprises, Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.

POSTMASTER: Send address changes to *2600*, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada—$15 individual, $40 corporate. Overseas—$25 individual, $55 corporate.

AN INTERVIEW WITH HUGO

by John Drake

Where did you get your alias from?

It was actually derived over a rather drunken lunch with the publisher, all that I had decided that it was to be a pseudonym, but I will explain genesis. Originally it was going to be Hugo Cornwell with an "E" rather than an "A" because David Cornwell is the real name of John Le Carre, a spy writer who I rather admire—he has also got a number of talented brothers and sisters. So the original thought was that it was going to be, in order to mislead the public, yet another member of a very talented family.

But at the time a number of the Elite hackers were operating under the name Pensanze, a SIG called Pensanze which had originally been called The Pirates of Pensanze for fairly obvious reasons. So Pensanze is in Cornwall, so that's how I came about. So we decided to call it Cornwall with an "A" and Hugo was chosen as a Christian name simply because I think it is one of the less likely names I could possibly have.

How did you start off as a hacker?

Not very deliberately. I got into communicating computers probably very early round about '78 and I just got very curious about what was going on in big computers and liked to drop in and eavesdrop and no one particularly seemed to mind and I never thought of it particularly as naughty or illegal but if I picked up a phone number or a password then I simply carried on collecting it. I ended up with a few sheets full of these things and I would pass them around to friends out of curiosity and it wasn't probably until '82 or '83 that I became aware that there were not just other people collecting [in a] similar sort of way but there was a proper culture outlet called Hacking and I said, "OK, well I suppose I am a hacker."

What did you do previous to hacking—did you have any other interests that were along the same line?

I guess I have been interested in what I call in the book the larger area of tech phreaking. In other words, making technology misbehave in the nicest possible way. I got interested in that when I was an undergraduate at Oxford and everyone I knew was interested in Phone Phreaking and that in fact one of the best phone phreakers was one of the dons and in the primitive sort of phone system that operated there you could really do a lot. So I was interested in that.

I certainly got interested in what we over here in England called bunker hunting. In other words, trying to find out secret sites used by the government and also by the U.S. government. There was partly a political motive in that but it was really rather a lot of fun.

I got interested also in the brief illegal citizen band radio thing that was going on in this country. I got a radio amateur license and I got also very interested in those parts of the radio spectrum that are not terribly well advertised. In most countries in the world, western world, you can buy books that tell you where all the various services lie. You can't in this country or you couldn't until very recently and I say [it] was great fun trying to work out the pattern of the allocation of the frequency bands and then using radio scanners [to] actually eavesdrop on them. You know although some of the stuff is now more widely known, there is a lot of the stuff that isn't known. There are a handful of people in this country who are really rather good at it.

How do the laws in the U.K. versus the U.S. encourage this type of investigation?

How do they encourage it? Well they discourage it really. It is done in two ways. First of all there is a lot less published in this country. We have got much tougher about what we publish. We don't have a Freedom of Information act. Anything that is generated by the government is deemed to be secret unless [it] has been specifically released for publication so there is a hell of a lot less information that is openly available. So there is that one aspect. The other aspect is that a lot of our laws are all enveloping in theory though they're widely ignored in practice. There is a contrast to the United States in particular. I know less about Canada and that is if you look specifically at hacking there is no specific anti-hacking legislation. You can be done for stealing telephone time if you look at telephone hacking, stealing electricity sometimes. You can be done for stealing CPU time on a computer and recently they have done to people for forgery which is basically using passwords to which they are not entitled and that case is going to appeal.

What was your motivation for writing "The Hacker's Handbook"?

The motivation was that I was asked to do it and it was very very easy. The way it happened was a man who was a hacker by interest and a publisher by profession wrote/scrawled a note on a bulletin board saying does anyone want to write a book on hacking and I wrote back not very seriously, in effect saying [you] cannot be serious, it can't be done. He wrote back, said I don't know, call me back and we will have a chat about it. I rang up, said/listed all the obvious things, why all the obvious reasons shouldn't be published and he sort of had a debate with me and at the end of it I felt maybe it could be done. I wrote him a synopsis within 24 hours. 24 hours afterwards he said it was terrific, would I mind waiting two or three days till he had his editorial meeting, but he wanted to do the book and at the end of all of that, you know within one week, beginning of the week I hadn't thought of writing the book, I hadn't thought of writing any book in fact and at the end of the week I actually had a contract.

So I would have never written a synopsis for the

book, I would have never hawked it around publishers but since there was the opportunity and I had already thought about the synopsis, I thought, well why not and I did. There was no great burning desire, there was an opportunity...so I went ahead and did it.

What has been the public/business and media response to your book?

There was a great deal of interest, the book was for several weeks on the Sunday Times Best Seller List so it was competing with some pretty popular items. I think it got popular interest largely because a reporter on the Sunday Times rang up the head of The Computer Security Squad at Scotland Yard [and] asked his comments. The man hadn't read the book but said sufficient for her to be able to headline a story "Yard Condemns Hacker Book". This immediately made the book appear very very important and very very serious and after that it took on a life of its own and I was from my amenity the whole thing with a great degree of amusement.

Those people who knew anything about hacking decided that it was not a very interesting book and I never thought that it would do but it obviously excited a lot of other interest. I think people created the book for themselves—they badly wanted a book about hacking, they wanted to make hackers into some sort of modern myth and my book happened to be around to capture all of that interest. Though there was a great deal of luck in it.

One of the effects of the Scotland Yard condemnation is that the books that hadn't been very widely distributed up till then, the original print run was very small, disappeared very rapidly from the bookshops and it created a further myth that the book had been banned in some way so everyone was rushing around like mad to get hold of them until about a few weeks when the book trade had recovered, copies were there, people grabbed it like crazy for fear that it [was] really going to disappear.

About two weeks after the book was published, a couple of guys were arrested for hacking the Prestel system and the newspaper reporters decided that one of those people was me, so there were headlines saying "Hacker Author Arrested" and things like that and again it wasn't true but it all helped sales.

It was really quite a phenomena and I do say to all hackers the attention that the book got was somewhat undeserved and I feel a little bit apologetic among serious hackers for sort of getting lucky.

In the first book you had a schematic for the Black Box. In the sequel it wasn't there. What was British Telecom's response to the book and how did it influence you in a sequel?

Well, the decision to take it out wasn't mine, it was the publishers, in fact it went in three stages. It was in the first edition the schematic was there complete with values for the various components and then gradually everything disappeared. I don't know that British Telecom did anything very much other than to condemn [the book] and what the publishers decided not unreasonably that things were getting a little bit hot and they [anticipated] trouble and removed the stuff so that they could show that they were being responsible. I think that is the way it happened. British Telecom said that they didn't approve of that sort of thing, that you know there are hackers on British Telecom's staff as you might expect so you know I think to answer to my certain knowledge a lot of people within British Telecom found it amusing and I also have reason to believe that some of the British Telecom Security people were not displeased about the book because it made everyone a lot more alert about the use of passwords.

There is some evidence also to show that quite a few of the books were actually sold either to computer security people or sold by them to, if you like, their customers in essence to say, "Look how easy it all is, read this book and be aware."

How would you say that U.K. hackers would be different from U.S. hackers?

I think that the difference is of sublety rather than of essence. I think there are two areas of difference. First of all my guess is that the majority of U.K. people, U.K. computer enthusiasts, that have modems probably acquired them about two or three years after the majority of U.S. equivalents.

That's really a question of how modems are sold. When I first got interested in computers, the only modems that were available were from British Telecom. You couldn't buy them over the counter in the shop and you had to buy them on rental and they were very expensive. If you had them, you either had fairly illicit ones, ones that had been modified from U.S. use and that was only of limited use or you had these very expensive ones which were registered with British Telecom.

So you got this two or three year gap. The second way I think is that again although it wasn't the case for me, most British enthusiasts, their first database they called into was going to be Prestel which is a video text system 75/1200 baud. The communication software that they had was for that as well. It meant that a lot of their hacking was either into Prestel or into systems which looked like it. Of course there was the university situation in the states where people would tend to be looking at microl clue de grass teletype services 300/300. I suppose that American hobbyists would call into The Source or into a BBS. After Prestel had been going for a bit then in the early eighties you started to get the BBS which people used 300/300. I

(continued on page 11)

some cosmos documentation

by Sir William

This article is intended for the serious COSMOS hacker. Many basic and fundamental functions of COSMOS were left out intentionally, such as logging onto COSMOS, etc. This is meant as an introduction in the operation and use of COSMOS (COmputer System for Mainframe Operations).

System Overview

COSMOS aids in the following functions:

- maintaining accurate records (for orders)
- processing work/service orders and keeping track of their status
- maintaining shortest jumpers on the MDF
- load balancing on the switching systems
- issuing reports

COSMOS can be run on a DEC PDP 11/45, PDP 11/70, or an ATT 3B20

Login

COSMOS identifies itself by its unique logon:

```
;LOGIN:
PASSWORD:
WC?
```

You can hack passwords, usually 4 alphanumeric characters—try SS0X, NA0X where X is a number. There are easier ways to get an account on COSMOS; i.e. social engineering a COSMOS support line. Wire Centers (WC) are 2 alphanumeric characters representing each central office.

Once you are on the system, you have full access to the COSMOS program. There is no security hierarchy while running the COSMOS program. Every user has full access to all the capabilities of COSMOS. However, there is a security hierarchy in the operating system. For example, not everyone can edit /etc/passwd on COSMOS—only a user with the root user ID 0:1 can do that. The shell privs of a user have nothing to do with COSMOS itself.

Transaction Code Format

To have COSMOS perform some action, you must enter a transaction. All transaction codes share a common format. In addition, there are specific rules for each transaction as specified in this article.

Generic Format

```
WC% XXX <CR>                WHERE XXX IS A SPECIFIC TRANSACTION CODE
   H item1/item2/etc <CR>   H-LINE
   I item1/item2/etc <CR>   I-LINE
   O item1/item2/etc <CR>   O-LINE
   R item1/item2/etc <CR>   REMARKS
```

- The H-LINE indicates a HUNT and is required in most transactions. Generally it refers to either order data, or inquiry and report data.
- The I-LINE indicates that INWARD movement is required, as when telephone service is being installed.
- The O-LINE indicates the transaction requires OUTWARD movement, as when a telephone line is disconnected.

To finish the transaction, type a "."—to abort, pound on the keyboard, or hit a Control-C. After a successful transaction has occurred, a double asterisk normally appears before the answer (**).

COSNIX

COSNIX is the operating system of COSMOS. Some COSNIX shell commands are the same as the UNIX (I assume familiarity with the UNIX operating system):

```
LS <pathname>  - list files
               - You can use this to find all other commands.
                 by listing /, and /bin.
CAT pathname   -   CATenate a file (View contents)
SH [-ceiknrstuvx] [arg]
   input/output commands : >, >>, <, <<, & digit
               - This invokes the COSNIX programming language.
               - The semantics of this command are too varied
                 to explain.  Suffice to say, it is almost
                 identical to the Unix "SH" command.
               - for example, sh command statements are:
                  - CASE word IN [pattern | pattern)..list;;]esac
                  - FOR name [IN word] DO list DONE
                  - IF list THEN list ... [ELSE list] FI
                  - list
                  - WHILE list DO list DONE
               - VARIABLES
                  - $# positional argument
                  - $? last executed command by the shell
                  - $! process number
                  - $HOME home directory
               - OTHER COMMANDS
                  - login [arg]
                  - SET [arg]
                  - wait
```

COSMOS Item Prefixes and Formats

Prefix	Definition	Format
ALT	Alternate	ALT YES or ALT NO
AO	Associated order	AO YES or AO NO
BAY	BAY (SXS) & (ESS)	BAY X (0,1,B,G)
BK	BANK (SXS)	BK X
BL	Bridge Lifter	BL XXXX
BTN	Billing Telephone Number	BTN XXX-XXXX
CA	Cable Number	CA XXXX
CAT	Centrex Treatment code	CAT XX
CC	Call Count	CC XX
CCF	Custom Calling Feature	CCF XXXXXX
CCS	CCS COUNT	CCS XX.X OR CCS XXX.X
CG	Control Group	CG X
CH	Choice (1XB)	CH XX
CP	Cable Pair	CP XXXX-XXXX
CR	Cable Pair Range	CR XXXX-XXXX-XXXX
CTX	Centrex Number	CTX XXXX
DD	Due Date	DD MM-DD-YY

that may be useful

DIP	Dip Option	DIP YES (NO)
DT	Due Time	DT MM-DD-YY
ECS	Equipment Class of Service	ECS XXXXX
ED	Enter Date	ED MM-DD-YY
EO	Error handling option	EO XX (CE, CW, SE, SW)
EQF	Equipment Features	EQF XXXX
FC	From Cable	FC XXXXX
FDD	Frame Due Date	FDD MM-DD-YY
FEA	Feature	FEA XXXX
	fields [1] R, T (ROTARY/TOUCHTONE)	
	[2] S (sleeve), X (range extension), N (no sleeve)	
	[3] E (essential), N (non essential)	
	[4] G (ground start), L (loop start)	
FR	MDF number	FR XX
GSO	Ground start option	GSO X (1,3)
HF	Hunt from telephone number	HF XXX-XXXX
HG	Hunt group	HG XX
HT	Hunt To telephone number	HT XXX-XXXX
KEY	Recent Change key	
LC	Output Line Count	LC XXXX
LCC	Line Class Code	LCC XXX
LOC	Location (2-digit frame)	LOC XXXXX
LS	List	LS NEW
LTN	Line Trunk Network (2ESS)	LTN XX
LV	Level (ESS)	LV XX
MAX	Maximum value of entity	MAX XX
MO	Month	MO XX
MOD	Module Number	MOD XXX
MIN	Minimum value of entity	MIN XX
NNX	Telephone Prefix Number	NNX XXX
NUM	Number of parameters	NUM XXXX
MRO	Message Register option	MRO YES (NO)
OC	Order Class	OC XXX
OD	Output Device	OD XXXX
OE	Office Equipment	
	NO. 1 ESS	OE XXX-XXX-XXX
	NO. 2 ESS	OE XXX-XXXX
	NO. 3 ESS	OE XXX-XXXX
	1XB	OE XXXX-XXX-XX or
		OE XXXX-XXXX-XX
	5XB	OE XXX-XXX-XX
	SXS	OE XXX-XXX
OP	Optional Printout	OP XXX
OPT	Party Assignment	OPT X (1-3)
ORD	Service Order Number	ORD XX.XX (25 MAX)
OT	Service Order Type	OT XX
PDF	Preferred MDF	PDF XX
PL	Circuit number (PRIVATE LINE)	PL XXXXXXXX
PRM	Parameter	PRM XXXXXXX
PRZ	Preferred Rate Zone	PRZ
PTY	Party number	PTY C
PWC	Print Work Code	PWC XXX
	(PBT, VBT, PCT, RCF, RBT, COM, USR)	
RC	Remarks on cable pair	RC XXXXXXXXXX
RCW	Recent Change Word	RCW XXXXXXX
RD	Release Date	RD XX-XX-XX
RE	Remarks on equipment	RE XX...X
REP	Reprint Option	REP Y
RLY	Relay	RLY XXXX
RMK	Remarks	RMK XX....XX
RT	Remarks on Telephone Number	RT XX.....XX
RW	Suppress recent change message	RW N
RZ	Rate Zone	RZ X
SC	Service Category	SC RES or SC BUS
SDF	Secondary MDF	SDF XX
SE	Special Equipment Number	SE XX...XX
SG	Segmentation	SG X
ST	Status of Load groups	ST XX
STO	Line Equipment Status	STO XX
STP	Cable Pair Status	
	[WK] working, [EX] Excluded, [FU] future	
STT	Telephone Number Status	STT XX
SW	Switch 1xb, ESS	SW X
SWC	Set Work Code	SWC XX
SWG	Switch Group	SWG X
TC	To Cable	TC XXXXX
TG	Telephone Number Range	TG XXX-XXXX-XXXX
TK	Trunk	TK XXXX-XXXX
TL	Premis TN list ID	TL XX....XX
TN	Telephone Number	TN XXX-XXXX
TP	Tie Pair	TP XXXX-XXXX
TR	Terminal Number	TR XXXX
TT	Telephone Number Type	TT X
TYP	Type (ESS, 1XB, 5XB, SXS)	TYP XXX
US	USOC	US XXXXX
USE	Usage	USE G or S
WL	Work Location	WL X, ALL, CPC, ADM, etc
WO	Work Order Number	WO XX....XX
WPN	Work Package Number	WPN XXX
WPT	Work Package Type	WPT XXX
ZN	Zone Number	ZN XXX

Cable Pair Status

WK	Working
SP	Special safeguard protection
SM	Special Safeguard Measures
DM	Designed + SSM
DP	Designed + SSP
DC	Designed Circuit
LI	Left in disconnect
DI	Defective
	I=1,9
RS	Reserved
UK	Unknown
EX	Excluded
SF	Spare
PC	Pending Connect
PD	Pending Disconnect

Line Equipment Status

WK	Working
OF	Company
TJ	Trunk and Junctor
TS	Test
MS	Miscellaneous
RS	Reserved
UK	Unknown
EX	Excluded
SF	Spare
PC	Pending Connect
PD	Pending disconnect
LI	Left in disconnect
FU	Future

Telephone Number Status

WK	Working
NP	Non published
AU	Auxiliary
OF	Company
TJ	Trunk and Junctor
TS	Test
MS	Miscellaneous
RS	Reserved
UK	Unknown
EX	Excluded
AV	Available
DO	Disconnect - Operator Intercept
DM	Disconnect - Machine Intercept
CO	Changed - Operator Intercept
CM	Changed - Machine Machine
SF	Spare
PC	Pending Connect
PD	Pending Disconnect

Service Order Types

NC	New Connect
CD	Complete Disconnect
CH	Change
F	From
T	To
SS	Suspension of Service
RS	Restoration of Service
R	Remark

Telephone Number Types

B	Business
C	Coin
O	Company
G	Good
X	Other
Q	Centrex

Service Order and Work Order Statuses

P	Pending
M	MDF completion only
A	PAO completion
C	final completion

Service Order--Secondary Status

P	Pending
J	Jeopardy
W	Withheld

(continued on page 14)

the telecom informer

BY DAN FOLEY

Cellular Phreaking

The future hinted in the December issue of *2600* is already here. Cellular fraud is becoming a concern of the CPC's (Cellular Phone Companies). Much fraud is from the same old source—the theft of cellular phones or even the entire car, resulting with the new "owner" making calls on the victim's cellular ID (and phone bill). Another form of fraud is from roamers (cellular users using their phones in a different city from where they signed up) who don't bother to let the CPC in the new city know their billing info. Roaming will become more prevalent as more people buy cellular phones and use them while they travel. However this form of fraud will soon become a thing of the past, as the CPC's are creating a national billing data clearinghouse which will ensure that bills will reach the right user. This clearinghouse will also (further in the future) allow someone to call a cellular telephone, and the call will be correctly routed to wherever in the United States the phone happens to be.

Of more interest to the readers of *2600* is something that is quickly growing and represents the most dangerous threat to CPC's billing. Spoofing another cellular user's ID isn't as hard as it seemed. Some of the more exotic schemes involve reading cellular ID's off of the airwaves as calls are being placed. Most CPC's don't even bother to encrypt the ID signals (and you don't even need to decrypt if the encryption algorithm doesn't include time and date stamping). But there is even a simpler method than using an "ether" box (so called because the box snatches ID's out of the "ether").

The easiest method by far needs the complicity of a cellular phone repair or installation shop. For many brands of phone the cellular ID is *not* in a ROM like "they" tell you, but instead is programmable. Motorola, for one, is supposed to have easy-to-follow instructions on programming their phone's cellular ID's inside the repair manual. And even if the ID is encoded in a ROM, you can just burn a copy. Rumor has it that cellular ROMs are already available on the black market. Perfect for your local terrorist to call in death threats and be untraceable, as the authorities would accuse the wrong person.

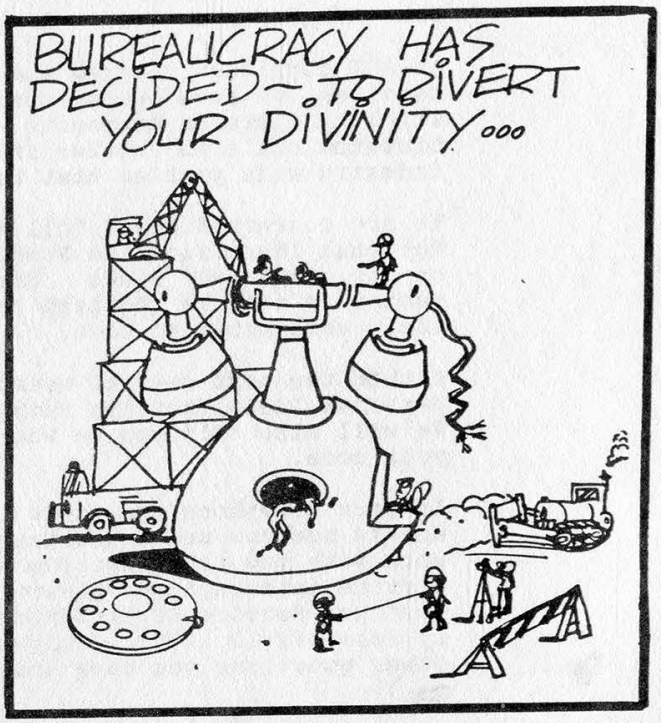
The Largest Cellular Companies

The largest cellular system in the world encompasses almost the entire Gulf of Mexico. On July 15 Coastel (sic) Communications began serving from Brownsville, Texas to Mobile, Alabama, with a switching office in Lafayette, Louisiana, and cell sites on offshore platforms out to about 160 miles from the coast. Coastel plans to target the oil business, fishing and other commercial marine operations. Airtime averages $1.00 a minute, rather expensive, but they do provide a specialized service. Cellular rates average about 60 cents a minute peak.

The largest cellular telephone company is now Southwestern Bell Corp. It bought out Metromedia's nonwireline rights for $1.65 billion. The FCC originally broke the cellular frequencies into three bands, giving one to the local telephone company (the wireline carrier), one to a nonwireline carrier, and saved one for the future. However the distinction has become academic as more RBOCs (Regional Bell Operating Companies) purchase cellular rights in other cities (with our local phone revenues we subsidize their investment in real estate, manufacturing, and all sorts of things having nothing to do with our dial tone). Southwestern Bell now competes against Nynex in Boston and New York, Bell Atlantic in Philadelphia and Baltimore/Washington, and Ameritech in Chicago and Dallas. It also got about 500,000 paging customers in nineteen cities. US West also competes against a fellow

(continued on page 16)


OH MIGHTY TELEPHONE MONOPOLY, YOU ARE GREAT AND MUCH TOO POWERFUL...


BUREAUCRACY HAS DECIDED - TO DIVERT YOUR DIVINITY...


IN THIS WAY YOU WILL NOT BE SO DIVINE AND THIS WILL GIVE THE PEOPLE WHAT THEY REALLY NEED!!!
A BIGGER HEADACHE!
NOT TO MENTION BAMBOZLED AGAIN!!
DAN HOLOSTR

Nasty Business

RCI Corporation
333 Metro Park
Rochester, New York 14623
716/475-8000

February 2, 1987

Dear RCI Customer:

As RCI continues to grow and expand its long distance services, we have become susceptible to a problem facing all long distance companies. Toll Fraud -- or making long distance calls on another individual's account -- is an industry-wide problem that has been increasing steadily.

We are concerned about Toll Fraud, and are adding 3-digit Personal Identification Numbers (PIN) to help prevent abuse on our customers' lines. Similar to a bank PIN code, customers will be required to dial their PIN code following their authorization code.

Within the next several weeks, you will receive your Personal Identification Number and dialing instructions. We will also tell you on what date you should begin using your code.

If your telephone equipment is programmed to dial RCI access numbers and authorization codes, we will have to work with you to re-program your equipment. To avoid any service interruption, please contact Judy Allen in our Customer Service Department, toll free, at 1-800-828-2733 by February 18, 1987. Judy will also be able to answer any other questions you have about this program.

Suzanne Crouse
Customer Service Assistant Manager
RCI Corporation

US SPRINT
8001 STEMMONS
DALLAS TX 75247

E-MAIL™

02/03/86 18:29:52 1063 323
02/03/86 18:43:37 MTAA

Attention: US Sprint Customer

A review of the number of calls made on each customer code is a part of our daily maintenance program. A recent review of your account shows a significant increase in calls as compared to your previous usage.

We were unable to contact you by telephone today to discuss this, and because we were concerned the calls being made on your code were unauthorized, we have suspended the code in question and will issue a new code as soon as you contact our Customer Service Department. Call us toll free at: 1-800-531-4646

We apologize for any inconvenience caused by this procedure and thank you for your continued business with US Sprint.

Sincerely,

US Sprint

WE SEEM TO BE GETTING LETTERS LIKE THESE EVERY COUPLE OF WEEKS. SOME, LIKE SPRINT, CAN'T EVEN GET THE DATE CORRECT!

CORNWALL (continued from page 5)

also think that because there were so many video text services, Prestel and type U H services to look at that on the whole British hackers weren't so much interested in big computer networks so it took them a bit longer to discover PSS and the various university networks like JANET (Joint Academic Network) and things like that.

In essence there is very little difference in the culture but a slight difference of preoccupation in terms of what they are looking for.

As a system, what do you think of Prestel?

You could go on and on and on about that. Prestel is extremely interesting as a matter of history. It had enormous ambitions, but its ambitions were all formed about the year 1975 which was eons before anyone visualized the home computer as being possible, so Prestel visualizes and suffers from it. People accessing computers via their television sets. Which is why you got a 40 by 24 character display, these rather curious graphics which was a function of the belief that memory was going to be unbelievably expensive and that 1k of display memory was really as far as you could go.

"...this idea that the hacker can somehow fight back, that's the reason why non-hackers admire them so much."

Also that the ordinary untrained person could never be expected to actually type words into a machine, you had to have all your commands being sole numbers. So you got this curious electronic card file type of structure and everything is available via pages or very simple numeric routing commands. Because Prestel is stuck with all of this sort of thing and if you like human knowledge about computers moved on fast, Prestel has to become more sophisticated, remain compatible with its 1975 format and a lot of the things you would want to be doing on a public access database, unbelievably clumsy. For example, you can order things, all the shopping and what have you, but you have to do it via a system called a gateway which is essentially, the way it works is that the gateway opens to receive a command string from you and it closes, the command string is processed in the remote computer, the gateway opens to give you the answer and closes again so on and so forth. Any more slightly more complicated interaction is unbelievably slow.

You could run an online service with view data as the front end processor, but it looks ridiculous, it behaves in a ridiculous format, so for certain types of services I suppose it's not too bad, it's like retaining a horse and buggy type of system when everyone is going around in gas driven internal combustion engines.

Can you see Prestel evolving from what it is now?

I don't think it will do, they're trying to make it evolve but I think it is going to remain as a historic curiosity. It's fairly [acceptable] in one or two industries, particularly the travel trade; it's quite useful for fast moving financial data. It will make very, very small movements but it will be relying on its installed user base. The way people are using it now is via emulators on personal computers. On my personal computer I obviously got video text, Prestel in other words type software and it's no effort to call into Prestel or any of the other online services.

I just can't see any electronic publisher saying, "Christ Almighty, we're really going to have to use this thing, this is wonderful." In fact, most electronic publishers nowadays publish in a variety of formats, they publish in an online format, they publish in a videotext format, and of course if their material is suitable they would also be thinking about publishing in a CD ROM type format and anything else that becomes available. It's merely a format and the decision to publish in it is "well, are there going to be enough people out there to make it worth my while?"

Electronic publishing in the form that you mentioned, how does it work over here, everything is online?

Well, you have a variety of systems, electronic publishing for the financial community, which is obviously the most lucrative area, is still very hardware bound in that if you want to get the service then the way the supplier wants to let you have it is that you have to buy his hardware and feed it down the leased line as well as getting the service.

That's the case with Reuters, they are under a lot of pressure to get rid of that and that is applied to most other services. You can hack into them because there is always exhibition/demonstration lines, dial-up lines available and then if you can fiddle with a personal computer system cleverly, you can get the services. Other forms are basically available online and you get it via PSS which is the British Telecom equivalent to Telenet or Tymnet.

(continued on page 15)

Some Suggestions

Dear *2600*:

I would like to thank you for your superb magazine. It would be a big plus this year if you could: 1) Show people what to do with a blue box now, before its death; 2) Teach how to hack a code with or without a computer like in your May 1986 issue; 3) Put out a list of exchanges like 950-1088 or 950-1033 etc. with the equivalent in 800 numbers and also tell us how many digits for their access code since it appears that some of them have more digits than originally.

I observed in Manhattan some fellows dial 950-1088, enter a valid access code plus a number (with the 517, 219, 601, or 505 area code and trunk it with 2600 hertz then KP 809 XXX-XXXX ST and reach their party in Santo Domingo. I wonder whether you could explain how they avoid CCIS.

In your May 1986 issue, page 3-38 there is an algorithm by Nynex Phreak which was one of the best. It was good for one month as described, but apparently some executive at MCI read that article and in June the message was changed to confuse people but with a little ingenuity you could still hack numbers according to the same explained principle. I had kept a list of codes which I used until December 24, 1986 on which day their computer invalidated all my codes. I would greatly like to know how many digits they use in their access code. Enclosed is a self addressed envelope so that you could provide me with a reply.

The Perpetrator

Here's your reply in a different envelope. We wish we had the time to reply personally to all of the letters we get but we simply do not.

We've published lists in the past of 950 numbers and 800 numbers as well. We'll be doing this again shortly. As far as how many digits are in a particular company's codes, it would be a full time job to keep track. Almost every day some long distance company somewhere changes their code pattern. Some even have more than one pattern. And quite a few have codes of varying lengths. If it's any help, our MCI codes are all five digits and our Sprint codes are nine. Beyond that it starts getting complicated.

We've printed full isntructions in the past as to how blue boxes are used. They do still work perfectly from a few locations to a few locations, but they become fewer every day.

Some Numbers

Dear *2600*:

Here are some phun numbers to call in the 716 area code:
688-3000 to 688-3040—University of Buffalo (VAX/CYBER)
878-5533 and 878-4611—Buffalo State Computing Service
874-3751—Computer Science
681-8700—BOCES
856-0720—Ticketron Buffalo
836-0000, 837-0000, 850-0000, 854-0000, 855-0000, 856-0000—weird tone.

I don't understand these numbers with weird tones and suffixes of 0000—is there any explanation to this? And does this happen in other area codes? Thanks.

Silver Bandit

Yes, it happens everywhere. Those are probably test numbers from the phone company. Why don't you call one and have it show up on your local bill? Then call the phone company and demand to know who that number belongs to and why it's on your bill. That's the easiest way.

On Cellular Phones

Dear *2600*:

Congratulations for beginning to publish articles on cellular telephones! The only thing wrong with the article

was the title—"a look at the *future* phreaking world". Cellular telephone phreaking is not in the future. To my knowledge, cellular telephone phreaking has been going on for about four years in at least one major metropolitan area. The lack of detailed information on cellular telephone phreaking in this publication has thus far placed *2600* in the dark ages.

Computer assisted blue boxing is still essentially the same as blue boxing in the dark ages of 1961. The same MF tones were used in 1961 and the phreakers were *very* successful. The advantages of using cellular telephones for phreaking and hacking instead of using land lines is outstanding. Cellular phones are the most immune to tracing even if used from a fixed location and it is virtually impossible to be nailed if you use one from a different location every time and for short duration or while you are travelling on a highway.

You mentioned in the article that for detailed info you should consult *EIA Standard CIS-3-A*. This publication has been outdated and has been replaced with *IS3-C*. Everyone interested in using cellular phones to their full potential should order all the publications on the subject from EIA, 2001 I Street NW, Washington, DC 20006, or you can call them at 202-457-4900.

The New Age Phreaker

We have yet to hear from a group of cellular phreakers, though we don't doubt they exist. By the way, have the Newspeakers among us begun saying celtels yet?

ANI Trouble

Dear *2600*:

The man who asked the question in the "Letter You Wrote" page, in the November issue, signed "Frustrated in Miami" regarding his ANI, evidently didn't read the Miami newspapers.

Some time ago, a school administrator named Johnny Jones was accused of stealing school funds. Unknown to him his telephone had been tapped.

This is an excerpt from the *Miami Herald* newspaper:

"Why, you may have wondered, did Johnny Jones continue to call his friend in Maryland despite the suspicion that his phone was tapped? Because, transcripts of those conversations disclose, Jones believed he had a secret number that told him whether his phone was tapped. Jones mentioned the number in almost every conversation with his friend and explained that if you call the number, your phone is clean. If you call and get a busy signal, your phone is tapped.

"Wrong, 'That's a test number for telephone installers,' says a Southern Bell spokesman. 'When they go out, installers have to hook up a lot of wires, and that number is a final checkpoint to see if they've got the right ones connected.' The spokesman says the phone company has lots of test numbers and a rumor for almost every one. 'As for the number Jones called, if you call it and get a busy signal, it simply means the line is busy, not that your phone is tapped.' "

The number, incidentally, isn't located in some supersecret vault in Langley, VA. It's in an electronic switching station off Red Road in South Dade. OK, OK. Call 1-200-666-6763.

If you have a letter to send to us, feel free to write. Don't ramble on for too long or we'll have to chop bits out. The address to write to is 2600 Letters Editor, PO Box 99, Middle Island, NY 11953.

 (continued from page 7)

Error Handling

Service order transactions interact with the user frequently. Each time the transaction is ready for new input, it will respond with an underscore at the beginning of the new line. This indicates that the preceding line is correct. If an error does occur, the transaction will respond with an error message and prompt for correction. When an error occurs, you have 4 choices: 1. Re-enter the entire field correctly; 2. Enter line-feed to ignore (checks rest of line); 3. Enter a ";" to disregard the present circuit; 4. Enter a "."—the transaction will disregard all input and exit.

H-LINE Inputs

H-LINE input for the service order trio SOE/CSA/TSA is being rigidly defined according to three categories. These categories contain fundamentally different types of order/facility information for the order.

Category 1: ORD, OT, DD, FDD, OC, DT, SG, EO, LC.

Category 2: US, FEA, CCF, CAT, BTN, SS, AO, RZ, FR, GP/CG, CTX/CG/MG/NNX, LDN, RTI.

Category 3: FW, RW.

Category 1 items are primary—once defined they cannot be changed by conflicting category 2 and 3 lines.

Service Order Transactions

Transaction	Definition
SOE	Service Order Input
TDZ	Telephone Number Assignment lists
LDZ	Line Equipment Assignment list
SOH	Service Order withheld
SOM	Service Order Modification
SOC	Service Order Cancellation
SOW	Service Order Withdraw
SCM	Service Order Completion by MDF
SCP	Service Order Completion by PAO
SCA	Service Order Completion Automatic
SCF	Service Order Completion for MDF automatic
SCI	Spare Cable pair inquiry
CDD	Change Due Date
BAI	Bridge Lifter Assignment Inquiry
LAI	Line Equipment Assignment Inquiry
NAI	Telephone Numbers Assignment Inquiry
TAI	Tie pair assignment Inquiry
EDZ	Facility Emergency Assignment list for backup
MAP	Manual Assignment Parameters
MAL	Manual Assignment list
TSW	Total Service Order Withdraw

Transactions Defined

SOE—Service Order Establishment:

Establishes a pending service order. The types of orders are: NC, CD, CH, F, T, SS, RS, R, RF. Reassociations are treated as change orders.

- H-LINES must contain ORD, DD, and OT. Optional facilities: FW, RW, FDD, AO, FR, SG, and either DT or OC.
- I and O LINES may contain US, FEA, CP, OE, TN, RZ, NNX, PL, TP, TK, BL, SE, CON, MR, BTN, RC, RE, RT, STC, STN, STO, CCF, LCC, and RTI.
- ESS orders requiring coordination by the recent change input center may be flagged with an input of "RW C".

Example of an NC (New Connect):

```
WC% SOE
H ORD NCXXXXXX/DD 01-01-86/OT NC/FDD 02-05-86/DT AM
_I CP XXXXX-XXXXXX/OE ?/TN ?/US 2FR/FEA RNNL
_.
```

Example of a CD (Complete Disconnect):

```
WC% SOE
H ORD CDXXXXXX/DD 01-01-85/OT CD
_O TN 534-1822
_.
```

Example of a CH (Change):

```
WC% SOE
H ORD CHXXXXX/OT CH/DD 01-01-86/TN 534-1822
_O TN 534-1822/STN CO
_I TN ?
_.
```

Example of SS (Suspension):

```
WC% SOE
H ORD SSXXXXX/OT SS/DD 01-01-86
_O TN 534-1822/SS SB
_.
```

TDZ—Telephone Number Assignments List:

List the indicated number of spare directory numbers for a NNX code, and directory number type.

- Up to 25 directory numbers can be specified, using the prefix LC.

Example:

```
WC% TDZ
H NNX 534/TT G/LC 7     (LC can be up to 25)
.
```

(continued on page 20)

CORNWALL

(continued from page 11)

There are also data-nets that use a Prestel like format but are not Prestel and you can get a number of services that way as well for example the equivalent to TRW for credit checking data is called CNN, that's available in the video text format. That doesn't come out via postal, it comes out via its own data network and there are other data networks with other services on them as well. So that's basically how it works.

Have you planned any future books on computer crime?

Well, I am writing a much more serious book at the moment called "Data Theft" which is intended for the chief executive officer of the CDO market and that is encouraging those people to the belief that they can't leave data security to a mere technical functionary. Though it is much more preoccupied with industrial espionage and fraud. It is not going to be in any way a tongue and cheek book. "Out of the Inner Circle" was alleged to be a book on computer security, but is manifested for hackers. This is a book on computer security and it is intended for chief executive officers and I don't think hackers would find it of any direct interest though I hope they are going to read it.

One of the things I do want to get over is this notion that most computer crime is committed by insiders, computer criminals are normally employed by their victims. I want to talk alot about police training or rather the lack of it and lack of responsive criminal code to cope with it. I still see that there is a lot of room for frolicking with technology and I really like to promote hacking to what I believe is its rightful place—something for a tiny, tiny minority to amuse themselves with, without actually causing any serious harm to anybody.

In the book "The Rise of the Computer State" the author put forward the premise that there is no defense against computer bureaucracy and having files built up on pretty well everybody, everything, and every move. Could you see hackers as a possible defense?

I have been asked this question in a slightly different form before. Not really, I think the mode of defense is that although these files can be built up, the files themselves are not necessarily terribly reliable.

One of the great problems with interpretive data is that they collect together so much information and so much gossip that although they can have it all on the screen in front of them they don't know whether it's terribly reliable. The value of the hacker I think is [a] somewhat dubious one in all of this. One of the reasons why I think there is so much room in people's hearts for the hacker is that they believe the hacker is going to provide that sort of defense which you were describing.

I actually wrote a piece for one of the papers about it [about] folk heroes arising, for example King Arthur is a very potent figure, Robin Hood is a very potent figure, and the potency of these things is that King Arthur is going to be [the] one and future king. Robin Hood, you know not a great deal is known about Robin Hood, but the great thing was that he stole from the rich to give to the poor and that probably is why he is remembered.

I think it is this idea that the hacker can somehow fight back, that's the reason why non-hackers admire them so much. I am afraid I don't believe that hackers are sufficiently good or sufficiently powerful or sufficiently able to combat that. I do think that every now and then though what a hacker can do is if he is very lucky, expose the stupidity [of] some of the power that is held on computers and maybe just enough that there is that element of defense that you're looking for.

But on the whole I would say the outlook for people/individuals in the computer age is not terribly good.

The Hacker's Handbook
by Hugo Cornwall
E. Arthur Brown Company, Alexandria, MN
169 pages
$12.95

Review by Roland Dutton

Strangely enough, this book actually lives up to its title. The author's stated purpose is to help the reader "grasp the methodology" and "develop the appropriate attitudes and skills, provide essential background and some reference material, and point you in the right directions for more knowledge." In this he succeeds, and in the meantime he gives us a lively and entertaining view of the world of British hacking.

The early chapters of the Handbook discuss the technical details of computer communications, the typical hacker's equipment, and the types of services or "targets" that a hacker might be interested in. The technical explanations are clear and accurate, and are neither too difficult for the beginner nor so simple that the seasoned system cruncher might not learn a few details from them. In general, the entire book appears to be an excellent beginner's manual, a very good intermediate manual, and enjoyable though certainly not indispensible reading for those who style themselves "advanced".

Two more chapters discuss "hacker's intelligence" and "hacker's techniques". Then computer networks and vidtex are discussed. The vidtex (also known as viewdata or videotext) chapter is interesting for American readers since none of those types of services are available here, and it's always interesting to know what's

(continued on page 21)

telecom informer

(continued from page 8)

RBOC, PacTel, in San Diego.

800 number allocation

It used to be that you could tell the geographical location of an 800-NXX number by the NXX part. XX2's were intrastate, XX7's were in Canada, and every prefix represented an area code. However, about five years ago AT&T introduced "Advanced 800 Service" which permitted any INWATS (Inward Wide Area Telephone Service) call to be routed anywhere in the US, and even to different destinations depending on both the time of day and where the caller placed the call. Thus 800-DIALITT would reach the nearest ITT billing complaint center during the day, and at night the call could instead reach a main office left open. The company has to pay for the normal 800 INWATS lines and then an extra couple of hundred a month for the "vanity" number and a few cents for each translation of end phone line by time or location.

Until Fall 1986 if your CO was switched over to equal access your 800 call was routed to AT&T no matter what your default carrier. But now your CO must route all 800 calls to MCI which have any of these "exchanges": 234, 283, 284, 288, 289, 274, 333, 365, 444, 456, 627, 666, 678, 727, 759, 777, 825, 876, 888, 937, 950, 955, and 999. US Sprint gets 728 and WUD Metrophone gets those to 988. The individual BOC's get the XX2 exchanges (as these are filled with intrastate WATS lines). More exchanges will undoubtedly be grabbed by other carriers as they begin to offer 800 service. I don't know what happens if your company's 800 number's exchange gets taken over by Bargin Bob's Telefone Kompany. Hopefully you get to keep the old provider, but this would really make it tough to route. Don't know what happens either if your clever little phone number "word" belongs to Bargin Bob, guess you gotta suffer. If your CO isn't equal accessable yet, it just kicks the call onto the nearest intra-LATA tandem site for the proper routing.

However, don't bother to remember this. When Bellcore finally finishes the new Advanced 800 service the INWATS buyer can route his or her incoming call through a different carrier depending on the originating point or the time of call, as well as sending it to a different company office. When this happens, all 800 calls will have to be sent to the nearest tandem switch and get routed based on all this info. The local telco will get the money for providing the routing service.

As far as I know only AT&T gets your 900 calls, which were never grouped according to geography. Trivia fact number 1: INWATS numbers in England (to the US. International INWATS further confuses the geographical determination) are of the form 0800-XX-XX-XX. Only AT&T provides this. Trivia fact 2: INWATS was not introduced in 1967 as stated in the December *2600*, page 3-95. The first *inter*state INWATS lines were in 1967, but intrastate INWATS started in 1966.

Airfone Update

The future of Airfone, the pay telephone for use on airline flights is in limbo. Airfone's experimental license expires at the end of 1987, and the FCC will not reconsider its January 1985 decision refusing permanent frequencies. Airfone expects to continue with over 300 plane phones and the 65 ground stations even though there is no provision for frequency allocation. Airfone hopes to be allowed to use cellular frequencies.

Remember the Greediest!

More Nasty Business

UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
U U N C L A S S I F I E D U
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU

ADMINISTRATIVE MESSAGE

ROUTINE

R: 071715Z SEP 86 ZYB

FM CNO WASHINGTON DC

TO NAVOP

BT
UNCLAS //N01600//

NAVOP 098/86
SUBJ: TELEPHONE CREDIT CARD FRAUD

1. TELEPHONE CREDIT CARD FRAUD CONTINUES TO OCCUR DESPITE AGGRESSIVE INITIATIVES BY COMMANDS AND THE HELP OF THE NAVAL INVESTIGATIVE SERVICE.

2. CONTRARY TO POPULAR BELIEF, THERE IS NO FREE LONG DISTANCE TELEPHONE SERVICE FOR OUR PEOPLE TO CALL ANYWHERE IN THE CONTINENTAL UNITED STATES OR OVERSEAS. NAVY PEOPLE USING UNAUTHORIZED CREDIT CARD NUMBERS ARE STEALING FROM COMMUNICATIONS COMPANIES AND BRINGING DISCREDIT TO THEMSELVES AND THE NAVY. MISUSE OF TELEPHONE CREDIT CARD NUMBERS OR FRAUDULENT USE OF AUTHORIZATION CODE NUMBERS WILL NOT BE TOLERATED. VIOLATORS ARE SUBJECT TO CRIMINAL PROSECUTION UNDER THE UCMJ AND CIVIL STATUTES, AS WELL AS ADMINISTRATIVE ACTION.

3. AN AGGRESSIVE PROGRAM OF EDUCATION, APPREHENSION AND PUNISHMENT IS NEEDED TO STEM THE TIDE.
BT

9977/230 MI 0317 230/19:57Z 071715Z SEP 86
CSM: 0285 CNO WASHINGTON DC

UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
U U N C L A S S I F I E D U
UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU

NEW DEVELOPMENTS

They've done it again. Our phone company has figured out a way to make a profit out of absolutely nothing. While we must commend them for their ever-present ingenuity, we must also point out that this is indeed the very last straw.

We all know how unjustified the charge for touch-tone service is. Touch tones make phone company equipment operate a lot faster, yet people can be fooled into thinking they're getting "access" to some kind of premium service. But the fact is that we all have access in the first place and the only way the phone company can change this is to invent a machine that makes your touch tones useless if you haven't paid. That's why touch tones work regardless of whether or not you pay for them on older phone systems. They're not sophisticated enough to operate that horrible machine. Remember—you're not actually paying for the service—you're paying for not being disconnected from the service.

The newest ripoff is a feature called "gold numbers". Do you remember the days when you could get a phone installed and ask if you could get a particular number? If the number was available, you'd be able to get it in most cases. Just like that. Well, you can kiss those days goodbye.

"For less than a quarter a day," the cheery little New York Telephone pamphlet says, "you could have a number that is easy to remember because of repeating or sequential digits. Or you might select any available 7-digit combination of numbers to suit your needs, perhaps trying for a number that translates into a word or phrase."

Isn't this brilliant? As if nobody had ever thought of selecting their own phone number before! And, since they were smart enough to come up with the idea, they've naturally earned the right to charge us $3 a month for one of these numbers or $6 a month for business customers. Maintenance charges, no doubt.

That's not enough? OK, here's some more. If the first three numbers you ask for aren't available (which doesn't necessarily mean they're being used), guess what happens? "A fee of $20 will apply for each 3-number search beyond the initial one." Twenty dollars just to apply for a number! And there's no guarantee you'll even get it! It could go on forever!

Obviously, the phone company is going to clean up on this if people are foolish enough to fall for it. One right after the other, we're seeing services that have always been free develop charges. While some changes in service are necessary because of the divestiture, this is certainly not one of them. It's time some nasty letters were written to our elected officials who have the power to do something about it.

Gold numbers indeed. Would anyone care to speculate on what they're going to try next?

Meanwhile there's an entirely new service that has sprung into being overnight. It's called PRS and it's being used by Mountain Bell and Pacific Bell. PRS stands for Personal Response System and means exactly the opposite. It seems that when you call up a directory assistance operator in those regions, the voice you hear saying, "Can I help you?" or "What city, please?" is actually a recording! Each operator records their own "greeting" and it plays when they pick up. This, according to the company, gives the operator some time to rest between calls. In fact, they like to refer to it as "the Pause that Refreshes and Satisfies." They say the customers just love it because the recording sounds so friendly and upbeat. Give us a break! It's just another way of turning those poor operators into machines. There's already a recording that gives the number, now there's one that picks up the phone! What's left?

2600 marketplace

DOCUMENTATION on electronic & digital PBX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 752B, Middle Island, NY 11953.

CELLULAR TELEPHONE INFORMATION WANTED. I will pay a modest fee for info which has not yet been published in 2600. Please describe the type of info that you have and name your price. Mr. B., P.O. Box 2895, Brooklyn, NY 11202.

MANUALS OR INSTRUCTIONS NEEDED for two modems labeled Dataphone Channel Interface. One has label on the outside that says: 44A2 Series 1, Data Mounting, SD-1D247-01-J23 and the other says: 44A2 DATA MTG, SD-1D247-01-J23, SERIES 1 83 MG 12. The boards on the inside are labeled: DAS 829B-L1A, SERIES 4, 81MG3 and DAS 829BL1A, SERIES 5, 84 MG 04. Send info to: P.O. Box 50346, Raleigh, NC 27650.

PRIVATE INVESTIGATOR wants to hear from 2600 readers who have electronic equipment he can buy cheap! Gaslamp Private Eye is into Electronic Counter-measures/TSCM in the trade parlance. 425 "F" Street, San Diego, CA 92101. (619) 239-6991.

TAP BACK ISSUES—complete collection, vol. 1-83 plus supplemental reports and schematics. Approx. 400 pages of quality copies sent via UPS or US Mail. $100 includes delivery. Send cash, check or MO (payable to PEI). Cash sent same day, others allow 4 weeks, to: Pete G., Post Office Box 463, Mt. Laurel, NJ 08054

HEY YOU! This is the chance you've been waiting for! A new service of *2600* Magazine. Got something to sell? Looking for something to buy? Or trade? This is the place! And it's free to subscribers! Just send us whatever you want to say (without making it too long) and we'll print it! And, if you send in the only ad we get, you'll get the entire page to yourself! Only people please, no businesses!
Deadline for March issue: 3/1/87.

 (continued from page 14)

Output example would look similar to this:

```
**EMERGENCY FACILITY ASSIGNMENT LIST 01-01-86
  RESERVED LINE EQUIPMENT
**NO SPARE LINE EQUIPMENT FOUND
  AVAILABLE DIRECTORY NUMBERS (7)
534-XXXX
534-XXXX, etc.
**TRANSACTION COMPLETED
```

SOW—Service Order Withdrawal:
Withdraws most recent version of a service order.
- Order number must refer to the latest version.

The H-LINE circuit ID
identifies the order. Valid circuit identifiers are: TN, XN, PL, CP, OE, and TK.
Example:

```
WC% SOW
H ORD NC-XXXXX/TN 534-1822
.
```

SCP—Service Order Completion by PAO:
Record in the Service Order File the completion of an order by PAO.
- Standard SXX H line input.

Example:

```
WC% H ord CDXXXXXX/TN 534-1822
.
```

SCA—Service Order Completion Automatic:
Enters final completion on all service orders which have been or are not required to be completed by the MDF, are not in a held or jeopardy status, and are due prior to or on the current date.
- Two due dates may be entered on the H-LINE; SCA will complete orders due on or between the dates. Additional options are OT (order type), ORD, and SG.

Example:

```
WC% SCA
.
```

(complete all orders on or before this due date)

Example2:

```
WC%SCA
H DD 01-01-86/OT NC
.
```

(complete all NC (new connect orders)

CDD—Change Due Date:
Change due date of a service or frame order
Example:

```
WC% CDD
H ORD CH-XXXXXX/TN 534-1822
I DD 01-01-86
.
```

Output Example:

```
**ORD CH-XXXXX  DUE DATE 01-01-86
```

NAI—Telephone Number Assignment Inquiry:
Provides from 1 to 25 spare telephone numbers compatible with the input specifications.
- Input is an H-LINE with the TN type and NNX or RZ entries. The status of the TN supplied will be modified to reserved if ST is specified on the H-LINE.

Example:

```
WC% NAI
H TT X/NNX 534/ST RS
.
```

(This shows first available spare in prefix 534.)

MAP—Manual Assignment Parameter:
Permits the PAO to establish the parameters that will constitute the PAO Open-of-Day report.

```
WC% MAP
I NNX 534/ECS 1R/EQF TNNL/LC 50, etc.
```

(for line equipment)

(for telephone numbers of type B, 10)

```
I NNX 534/TT B/LC 10
```

(Thanks to Loki, Evel Eye, and Sir Galahad for their contributions.)

In the future we will be devoting more time to just what COSMOS means to the average person and how it can effect and disrupt their lives. There are many other computer systems that are capable of doing all kinds of other things to your personal lives. We welcome information and comments on them all.

Write to 2600, PO Box 99, Middle Island, NY 11953-0099. Or call the office at (516) 751-2600.

(continued from page 15)

going on elsewhere. As one might expect from a British author, the discussion of computer networks centers around the British public data networks, which are similiar to Telenet or Tymnet.

And for those hackers who have too many security officers chasing after them, one chapter discusses "radio computer data", also known as radio teletype or RTTY. This is not really hacking, but just an interesting way to use your computer when you're not moving satellites with tank parts ordered from TRW. You need a short wave receiver and an interface (which starts at $40), and you will be able to tune in various stations that use the international short-wave bands for transferring computer data. Sample listings in the book show a news bulletin about the Enver Hoxha Automobile and Tractor Combine in Albania, and some typical amateur radio conversations.

Every chapter always has one or two ideas or techniques that the capable hacker can use to expand his or her horizons. Here's one fun idea that rarely gets discussed, under the heading of "Hardware Tricks":

"For the hacker with some knowledge of computer hardware and general electronics, and who is prepared to mess about with circuit diagrams, a soldering iron and perhaps a voltmeter, logic probe, or oscilloscope, still further possibilities open up.

"One of the most useful bits of kit consists of a small, cheap radio receiver (MW/AM band), a microphone, and a tape recorder. Radios in the vicinity of computers, modems, and telephone lines can readily pick up the chirp chirp of digital communications without the need of carrying out a physical phone tap. Alternatively, an inductive loop with a small low-gain amplifier in the vicinity of a telephone or line will give you a recording you can analyze later at your leisure." [An inductive loop is a long piece of wire wrapped around in circles placed next to the line that you want to listen to. A typical inductive loop is the suction cup microphone that sticks to a telephone handset and records the conversation without being physically attached to the line.]

Overall, *The Hacker's Handbook* is a good book for those hackers who want to broaden their horizons, or who just need some new ideas. Hackers on both sides of the pond will get a better understanding of the magical machinery that places all this tintillating telecommunications within our grasp.

Automatic Teller Machines III
by John J. Williams, MSEE
Consumertronics Co.
P.O. Drawer 537
Alamogordo, NM 88310
$25.00

Review by Lord Phreaker

Automatic Teller Machines (ATM's) are the wave of the future in banking. Projections aim at 500,000 ATM's and Point of Sale terminals (POS) in place by the year 2000. By 1990 there will be $550 billion worth of ATM transactions per year. ATM's are becoming a major force in the banking industry, with more than 58 million Americans using them. But along with the added convenience and lower costs to banks of using ATM's, crimes involving these machines have grown enormously as ATM use expands.

Reported ATM crime in 1983 was between $70 and $100 million, and estimates run as high as $1 billion. These figures don't include muggings and other crimes directly against ATM users. With $50,000 in a newly refilled ATM, "a veritable cookie jar," these machines are becoming the focus of criminals. ATM fraud soon will become a major criminal activity.

John Williams begins his pamphlet with a series of apocalyptic warnings about the repercussions of this boom in ATM fraud. According to his "Background Information", John Williams is very convinced of the danger this growing area of fraud poses to the American public. His apocalyptic visions get carried to extremes, as he states that "I strongly feel that all forms of EFT [Electronic Funds Transfers, which include ATM's] are instruments of Satan

and must be destroyed to prevent enslavement by the Antichrist." These dire forebodings are interspersed throughout the text, complete with references to Big Brother. Williams also dislikes the banks and other capitalistic enterprises. He claims it is in the banks' best interests to suppress stories of ATM fraud losses. ATM transaction costs are much less than those dealing with live human tellers. In addition, Williams claims that once banks have gotten the public to prefer using ATM's, they will raise charges to the customer for ATM transactions. He also warns against the "ominous risks to our freedoms and privacy" as the ATM invades the home. Although these claims certainly make entertaining reading, they detract from the seriousness of the work and make it too easy to dismiss. However, once one gets beyond these ravings one realizes that there actually is some useful information here.

One area where the book excels is the section dealing with protecting oneself from fraud. Many of the suggestions are common sense, but many people don't even think of using them. Williams is especially concerned about violent crimes against ATM users by muggers. For example, he suggests that one never withdraw funds between 10 and midnight, as criminals can then make two days of maximum withdrawals with your card. Williams also addresses your legal rights. If a violent crime occurs within the ATM lobby, you can probably successfully sue the bank for improper safety measures. The section on how many ATM scams work is helpful, as most of them involve somehow tricking the victim into revealing his PIN. He also lists several warning signs of ATM fraud in progress or about to happen so one can avoid becoming another victim. The section on protecting oneself from fraud perpetrated by bank employees as well as more common criminals is indeed valuable, as is the discussion on EFT laws.

The technical section is interesting, but not very useful. Williams focuses on the Diebold ATM, which accounts for about 45% of installed ATM's, but one wonders if the information is out of date or only applies to one model. There is a discussion of several other models as well. He does enter into a useful and interesting explanation of ATM card magnetic strip formats, as well as encryption schemes. This really is the most interesting and informative part of the entire booklet, as he in depth discusses PIN encryption and data formats. The technical sections on how ATM's and ATM networks operate is also interesting, although not specific enough.

If you bought the book with the hope of finding out an easy way to break into an ATM machine, forget it. Most of the methods are sufficiently vague that you would have to do much more investigation on the topic anyway (luckily for the rest of us). Many of the physical attack methods are just the same as for pay phones (or any other armored object, though surprisingly many ATM's are only fire resistant, not burglar or tool resistant), and are really innately obvious. Many of the successful methods used in the past are due to programming mistakes which probably have been repaired. ATM security seems to be a rapidly evolving field, and major holes are patched as soon as they become apparent. The section on computer related break-in methods was especially vague, and much of the material was too generalized, and could be applied to any computer crime.

When one comes to the end of the booklet one wonders if it was worth the cost. Twenty-five dollars is a lot for fifteen pages (plus a three page feedback questionnaire) of badly xeroxed ravings. Each page, however, is two columns of very small print, containing some information of worth, much of which is impossible to find from any other source. The diagrams aren't extremely helpful, mainly being cartoons and publicity shots. Williams often plugs his other books in the work, as well as America's Promise Radio, which is distracting (admittedly, he also plugs *2600* as "the best source on phone and computer phreaking"). This could be a better investment if the ravings were removed along with a lot of the extemporaneous material. It isn't especially useful to scan through columns of clippings telling that so-and-so stole such-and-such amount somewhere. Many of the clippings really have nothing to do with ATM fraud, and are merely cute filler. My suggestion to the author for *Automatic Teller Machines IV* is to cut out much of the diatribes which detract from the seriousness of the topic.

ATTENTION

These are the new prices now in effect. You can still save money and hassles by renewing for two or three years.

$15 ..... 1 year subscription or renewal
$28 ..... 2 year subscription or renewal
$45 ..... 3 year subscription or renewal
$40 ..... 1 year corporate subscription or renewal
$75 ..... 2 year corporate subscription or renewal
$110 ..... 3 year corporate subscription or renewal
$25 ..... overseas subscription or renewal (1 year only)
$55 .. overseas corporate subscription or renewal (1 year only)
$260 ..... lifetime subscription

Back issues have new prices too. They are:

$25 ..... 1984, 1985, or 1986 issues (12 per year)
$50 ..... Any two years
$75 ..... All three years (36 issues)
(Overseas orders add $5 for each year ordered)

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

CONTENTS

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

SAVE YOUR ADDRESS LABEL FOR LOGIN
TO THE NEW PRIVATE SECTOR BULLETIN BOARD!
(201) 366-4431